Les maisons intelligentes le sont-elles en termes de cyber-sécurité ?

L'ENISA publie aujourd'hui le Paysage des menaces et guide des bonnes pratiques pour les maisons intelligentes et les media convergents, une contribution à la réalisation des objectifs de la Stratégie de cyber-sécurité de l'Union Européenne. L'étude a pour but d'identifier les défis et risques en termes de sécurité, ainsi que les mesures requises en termes de technologies émergeantes dans les maisons intelligentes, en fournissant une approche spécifique, et un aperçu du stade actuel de la cyber-sécurité dans ce domaine émergent.

Afin d'établir ce rapport, un groupe d'experts informel a été créé pour collecter des contributions à différents stades de ce projet. De plus, l'étude prend en compte des sources publiques valables et fournit un Paysage des menaces par thème dans le domaine des maisons intelligentes.

Dans le cadre de l'étude, des facteurs de menaces ont été identifié révélant différentes sources de vulnérabilité. Les cybercriminels sont identifiés comme la catégorie de menace la plus importante et la plus hostile, tandis que les potentielless violations de maisons intelligentes sont considérées comme élevés, dû au nombre croissant d'appareils et de maisons intelligents et plus particulièrement de medias connectés. De plus, de nombreux facteurs économiques génèrent des vulnérabilités dans le système de sécurité, tandis que des choix de conception peuvent entrer en concurrence avec des questions de choix et de commodité.

De nombreux risques seront de type socio-technique, du fait de l'importance et de la variété des informations personnelles qui peuvent être captées et téléchargées, et produiront des données sur des activités précédemment non-enregistrées, avec un lien étroit entre les individus et leur environnement. De plus, les intérêts des différents propriétaires d'actifs dans les maisons intelligentes ne sont pas nécessairement les mêmes et ont même des chances d'être en conflit, créant un environnement complexe pour la cyber-sécurité.

D'un autre coté, les medias et télévisions connectés posent des questions de sécurité en terme de connectivité, de fonctionnalité intégrée, d'opacité et d'incompatibilité avec les approches traditionnelles en termes de sécurité de l'information, ainsi que des questions de respect de la vie privée, d'accès et de droit d'auteur. Les dispositifs de medias connectés sont probablement les premiers appareils intelligents introduits au sein de nombreux domiciles particuliers, et seront sans doute le terrain de nombreux problèmes de sécurité identifiés.

Toutes les maisons intelligentes ne sont pas construites de la même façon, du fait de multiples trajectoires qui résultent de leurs propres particularités, problèmes communs et vulnérabilités en termes de sécurité. Comme dans plusieurs autres domaines des technologies de l'information, appliquer une sécurité de l'information basique peut augmenter de façon significative toute la

sécurité dans le domaine des maisons intelligentes.

Les bonnes pratiques dans ce secteur impliquent de prendre en compte le design des maisons intelligentes comme un système, de considérer de manière prudente la sécurité des designs de maisons intelligentes basés sur le cloud, d'appliquer une structure d'isolation particulière (comme développé dans les voitures intelligentes), et de garder les logiciels critiques éloignés des applications non-critiques, des réseaux et des communications sur les mesures de sécurités. Des approches similaires appliquées aux grilles intelligentes peuvent se révéler applicables dans le contexte des maisons intelligentes.

Le directeur exécutif, Udo Helmbrecht a commenté : *« Les maisons intelligentes sont un point de contact important entre la technologie de l'information en réseau et l'espace physique, et par conséquent apportent en même temps des risques de sécurité issus des contextes virtuels et physiques. Identifier les cyber-menaces est crucial pour la protection des maisons intelligentes et est par conséquent un élément clef pour assurer leur déploiement. »*

Pour le rapport entier : Paysage des menaces pour les maisons intelligentes et les media convergents

Pour toute demande d'interviews et pour contacter les auteurs, merci d'écrire à resilience@enisa.europa.eu

Pour toute demande de presse press@enisa.europa.eu.

Notes aux rédacteurs :

Figure 1 : Aperçu des biens des maisons et médias intelligents p.11

Figure 2 : Aperçu des menaces possibles pour des biens de maisons intelligentes p.13

Association entre les menaces et les biens de maisons intelligentes p.34

Tableau 1 : Implication des facteurs de menaces dans les menaces p.38

Tableau 3 : Bonnes pratiques contre les catégories de menaces p.51

Paysage des menaces annuel de l'ENISA **2014**, **2013**, **2012**

Paysage thématique des menaces ENISA :

Paysage des menaces et bonnes pratiques pour les infrastructures internet (2014)

Paysage des menaces pour grilles intelligentes et du guide des bonnes pratiques (2013)